(12) UK Patent Application (19) GB (11) 2 379 040 (13) A

(43) Date of A Publication 26.02.2003

(21) Application No 0120391.8

(22) Date of Filing 22.08.2001

(71) Applicant(s)
International Computers Limited
(Incorporated in the United Kingdom)
26 Finsbury Square, LONDON, EC2A 1SL,
United Kingdom

(72) Inventor(s)
Nicholas Peter Holt
Matthew Roderick

(74) Agent and/or Address for Service
Fujitsu Services Limited
Observatory House, Windsor Road,
SLOUGH, Berkshire, SL1 2EY,
United Kingdom

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition V)
G4A AAP A23B A23X

(56) Documents Cited
EP 1107089 A1 **WO 1995/019593 A1**
US 6259909 B

(58) Field of Search
UK CL (Edition T) **G4A** AAP
INT CL[7] **G06F** 1/00
Other: **ONLINE: WPI, EPODOC, JAPIO, TDB, INSPEC**

(54) Abstract Title
Controlling user access to a remote service by sending a one-time password to a portable device after normal login

(57) A method is described for controlling user access to a remote service over a network, such as the Internet. In an initial log-in procedure, the user enters a user name and user password over the network, and the service validates the combination of the user name and user password. If validation of the combination of the user name and user password is successful, the service sends a one-time password to the user via a wireless messaging service, to a portable device personal to the user. The portable device may be the user's mobile phone and the message may be an SMS message. A supplementary log-in procedure is then performed, in which the user enters the received one-time password over the network, and the service validates the one-time password. If validation of the one-time password is successful, the user is allowed to access the service over the network.

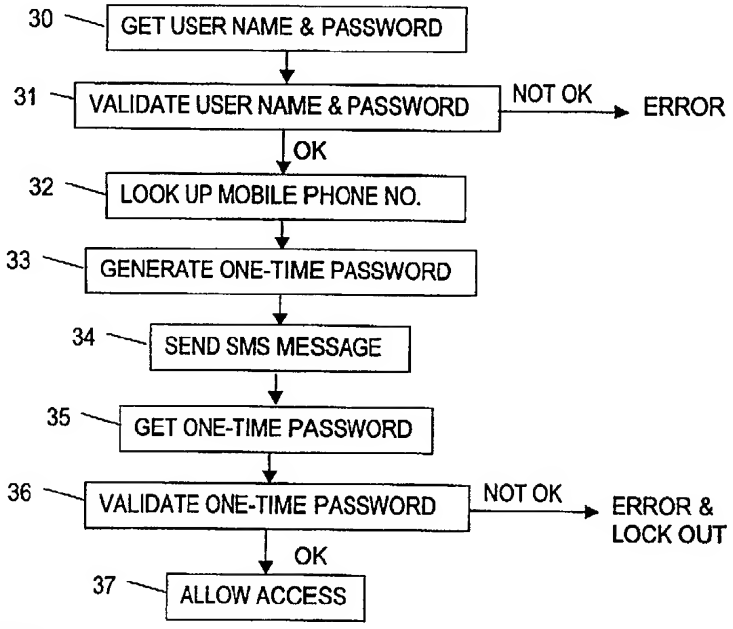

FIG. 3

GB 2 379 040 A

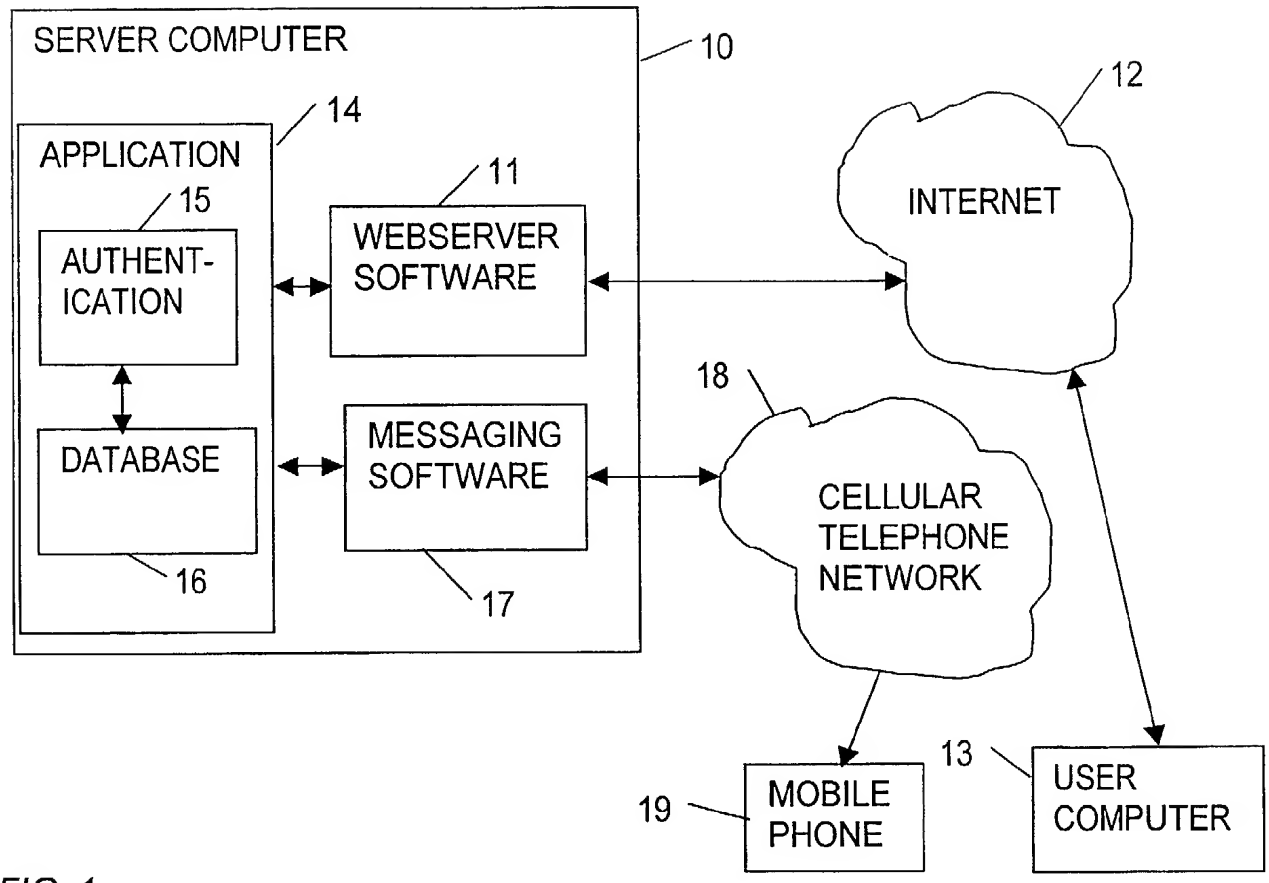
SERVER COMPUTER
10
12
14
APPLICATION
11
INTERNET
15
AUTHENT-
ICATION
WEBSERVER
SOFTWARE
18
DATABASE
MESSAGING
SOFTWARE
CELLULAR
TELEPHONE
NETWORK
16
17
13
19
MOBILE
PHONE
USER
COMPUTER

FIG. 1

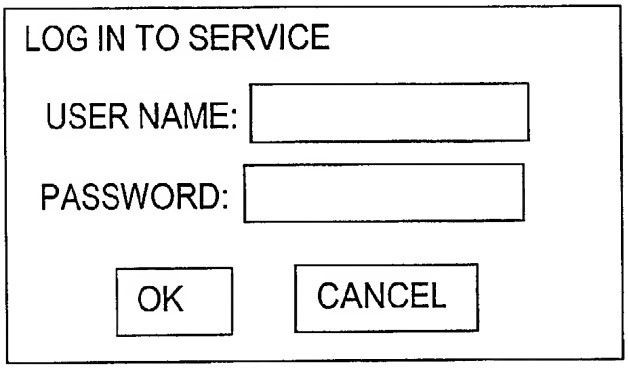
LOG IN TO SERVICE
USER NAME:
PASSWORD:
OK
CANCEL

FIG. 2

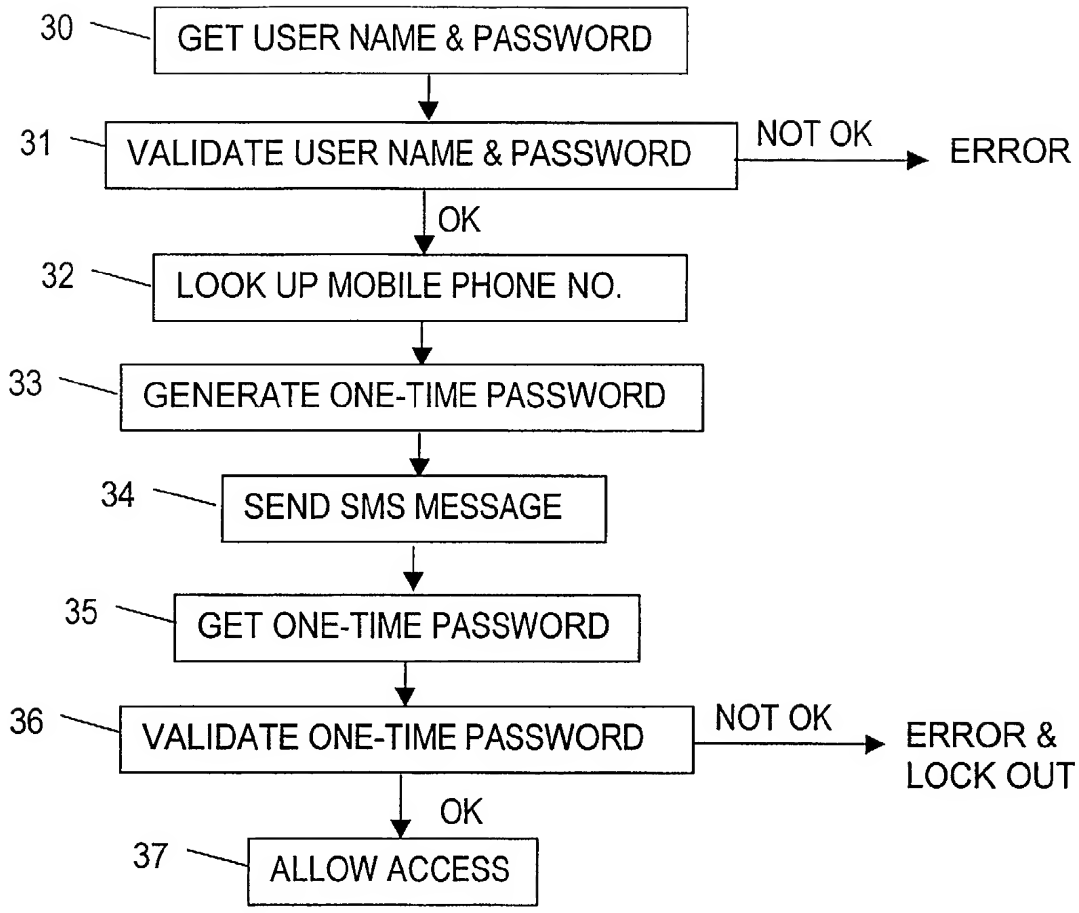
30
GET USER NAME & PASSWORD
31
VALIDATE USER NAME & PASSWORD
NOT OK
ERROR
OK
32
LOOK UP MOBILE PHONE NO.
33
GENERATE ONE-TIME PASSWORD
34
SEND SMS MESSAGE
35
GET ONE-TIME PASSWORD
36
VALIDATE ONE-TIME PASSWORD
NOT OK
ERROR &
LOCK OUT
OK
37
ALLOW ACCESS

FIG. 3

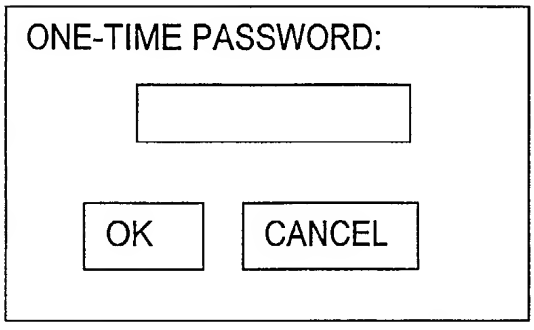
ONE-TIME PASSWORD:
OK
CANCEL

FIG.4

System for controlling user access to a remote service

Background to the invention

This invention relates to a method and apparatus for controlling access to a remote service, such as a service provided over the Internet or an in-house intranet.

One common way of controlling access to a remote service is to require the user to log in to the service using a user name and password. However, a problem arises if the user attempts to log in from some non-trusted device, e.g. from some other organisation's site, or from a public device such as a kiosk or an Internet cafe. In this case, there is a danger that the user name/password combination may be intercepted by the device. The actual session can be protected, e.g. using https/SSL, but the password is still vulnerable to software on the device that, for example, may log keystrokes. There is then the danger that the log-in sequence can be subsequently replayed, allowing a non-authorised user to access the service.

The object of the present invention is to provide a system for log-in to a remote service which overcomes this problem of passwords being intercepted and replayed.

Summary of the invention

According to the invention, a method of controlling user access to a remote service over a network comprises:
(a) performing an initial log-in procedure, in which the user enters a user name and user password over the network, and the service validates the combination of the user name and user password;

(b) if validation of the combination of the user name and user password is successful, sending a one-time password to the user via a wireless messaging service to a portable device personal to the user;
(c) performing a supplementary log-in procedure, in which the user enters the received one-time password over the network, and the service validates the one-time password;
(d) if validation of the one-time password is successful, allowing the user to access the service over the network.

In a preferred embodiment of the invention to be described, the network is the Internet, the portable devices are cellular mobile phones, and the one-time passwords are delivered using the short messaging service (SMS).

It will be seen that, by using this method, even if the log-in sequence of user name, user password and one-time password is intercepted and logged, it cannot be subsequently replayed by an unauthorised user. Security depends on the user both knowing the correct user name and user password, and being in possession of their own portable device.

Brief description of the drawings

Figure 1 is a schematic block diagram of a distributed computing environment for providing a secure service to a number of users.

Figure 2 shows a form for entering user name and user password.

Figure 3 is a flow chart of a log-in process.

Figure 4 shows a form for entering a one-time password.

Description of an embodiment of the invention

One system for allowing a user to log in to a secure service will now be described by way of example with reference to the accompanying drawings.

Figure 1 shows a server computer 10 which runs conventional web-server software 11, and can be accessed over the Internet 12 (or over an in-house intranet) by a number of user computers 13. The user computers may be conventional personal computers (PCs), running conventional web-browser software.

The server computer 10 also includes application software 14 for providing a secure service. The exact nature of the secure service forms no part of the present invention and so will not be described in detail. The application software 14 includes authentication software 15, for controlling user log-in. The authentication software uses a secure database 16, containing a user name, user password (typically one-way encrypted), and mobile phone number for each registered user.

The server 10 also includes messaging software 17, which has access to the public cellular telephone network 18, and can send text messages to users' mobile phones 19 using the short messaging service (SMS).

Figure 3 shows the log-in process which occurs when a user wishes to access the secure service.

(Step 30) In response to the user typing in the URL of the server, the server returns an initial log-in page to the user's browser, as illustrated in Figure 2. The log-in page requests the user to enter his or her user name and user password. When

the user clicks on the OK button, these are returned to the server. This dialogue is typically secured by using https/SSL.

(Step 31) When the server receives the user name and user password, it validates the user name/password combination, using the information stored in the secure database. If the validation fails, the server returns an appropriate error message to the user. However, assuming that the validation is successful, the server proceeds as follows.

(Step 32) The server looks up the user's mobile phone number in the secure database.

(Step 33) The server then generates a random one-time password, and stores it memory.

(Step 34) The server then sends an SMS message to the user's mobile phone, containing the one-time password.

(Step 35) The server than sends a form to the user's browser, as illustrated in Figure 4. This form requests the user to enter the one-time password. (Note that this form may be received by the user before the SMS message, in which case the user must wait at this point until the SMS message is received). When the user enters the one-time password from the SMS message, and clicks on the OK button, the one-time password is returned to the server.

(Step 36) The server then validates the one-time password against the stored value. If the validation fails, the server returns an appropriate error message to the user, and initiates a predetermined (configurable) lock-out period, to prevent machine-based attacks on the service.

(Step 37) Assuming that the validation of the one-time password was successful, the server then returns an initial service page (home page) to the user, and the user can now start using the service.

It can be seen that the one-time password is different for each log-in, so that even if the log-in sequence of user name, user password and one-time password is intercepted and logged, it cannot be subsequently replayed by an unauthorised user. Security depends on the user both knowing the correct user name and user password, and being in possession of their own mobile phone.

Another advantage of the system described above is that if some unauthorised person tries to use a user name and password, the user will receive an unexpected SMS message. This will alert them to the fact that someone is trying to gain access to their account, and allow them to immediately inform the service provider.

Some possible modifications

It will be appreciated that many modifications may be made to the system as described above. For example, instead of using SMS messages, other forms of text messaging, or even voice messaging, may be used to deliver the one-time passwords. Also, although the system described above was an Internet-based system, the invention would be equally applicable to networks based on other protocols. In another possible modification, instead of generating the one-time passwords randomly on demand, as described above, a set of one-time passwords may be generated in advance, and stored securely in the server until required.

Claims

1. A method of controlling user access to a remote service over a network, the method comprising:
(a) performing an initial log-in procedure, in which the user enters a user name and user password over the network, and the service validates the combination of the user name and user password;
(b) if validation of the combination of the user name and user password is successful, sending a one-time password to the user via a wireless messaging service to a portable device personal to the user;
(c) performing a supplementary log-in procedure, in which the user enters the received one-time password over the network, and the service validates the one-time password;
(d) if validation of the one-time password is successful, allowing the user to access the service over the network.

2. A method according to Claim 1 wherein said network is the Internet.

3. A method according to Claim 1 or 2 wherein said portable device personal to the user comprises a mobile telephone.

4. A method according to Claim 3 wherein said wireless messaging service comprises a text messaging service.

5. A method according to any preceding claim wherein said one-time password is generated randomly on demand.

6. A method of controlling user access to a remote service over a network, substantially as hereinbefore described with reference to the accompanying drawings.

7. Computer apparatus for providing a remote service over a network, the apparatus comprising:
(a) means for prompting a user to enter a user name and user password over said network;
(b) means for validating the combination of the user name and user password entered by the user;
(c) means for sending a one-time password to the user via a wireless messaging service to a portable device personal to the user, if validation of the combination of the user name and user password is successful;
(d) means for allowing the user to enter the received one-time password, over said network;
(e) means for validating the one-time password entered by the user;
(d) means for prompting the user to access the service over the network, if validation of the one-time password is successful.

8. Computer apparatus according to Claim 7 wherein said network is the Internet.

9. Computer apparatus according to Claim 7 or 8 wherein said portable device personal to the user comprises a mobile telephone.

10. Computer apparatus according to Claim 9 wherein said wireless messaging service comprises a text messaging service.

11. Computer apparatus according to any of Claims 6 to 10 wherein said one-time password is generated randomly on demand.

12. Computer apparatus for providing a remote service over a network, substantially as hereinbefore described with reference to the accompanying drawings.

INVESTOR IN PEOPLE

Application No: GB 0120391.8
Claims searched: 1-12

Examiner: Paul Jefferies
Date of search: 28 March 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A (AAP)

Int Cl (Ed.7): G06F 1/00

Other: ONLINE: WPI, EPODOC, JAPIO, TDB, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP1107089 A1	(CONNECTOTEL) See whole document.	1-12
X	WO 95/19593 A1	See figure 1, abstract and pages 7, 8.	1-12
X	US 6259909 B1	(RATAYCZAK et al.) See column 6, line 59 to column 7, line 47 and figures 5, 7.	1-12

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.